ABSTRACT OF THE INVENTION

A method, system, and computer program product for providing consistent, end-to-end protection within a computer network for user datagrams (i.e. packets) traveling through the network. The network may comprise network segments that are conventionally assumed to be secure (such as those found in a corporate intranet) as well as network segments in non-secure networks (such as the public Internet or corporate extranets). Because security breaches may in fact happen in any network segment when datagrams are unprotected, the present invention discloses a technique for protecting datagrams throughout the entire network path by establishing cascaded tunnels. The datagrams may be exposed in cleartext at the endpoints of each tunnel, thereby enabling security gateways to perform services that require content inspection (such as network address translation, access control and authorization, and so forth). The preferred embodiment is used with the "IPSec" (Internet Protocol Security Protocol) and "IKE" (Internet Key Exchange) protocols, thus providing a standards-based solution.